REMARKS

A. In paragraph 13 (page 3) of the Office action, the Examiner erroneously objects to the disclosure based on typographical errors in the Amendment filed on 08/06/03. Since the typographical errors in the Amendment are not part of the "disclosure," then the objection makes no sense and is untenable. The Applicant takes note of the typographical errors in the Amendment as pointed out by the Examiner, and agrees with the Examiner's assessment as to the correct meanings intended.

Accordingly, the objection should be withdrawn.

B. Claims 70-94 were rejected under 35 U.S.C. §112, second paragraph based upon a number of apparent deficiencies kindly noted by the Examiner. Accordingly the above amendment is believed to correct for actual deficiencies not discussed below.

In paragraph 14 bridging pages 4, 5 and 6, the Examiner erroneously holds various terms and phrases to be indefinite. The various terms and phrases can be found in numerous "valid" patents, and the Examiner has offered no new MPEP guideline, or Case Law, supporting the Examiner's holding of indefiniteness.

For example, the Examiner offers an example of the term "for" in such phrases as "for generating", "for transmitting," etc. If the Examiner holds that such use of the term "for" is indefinite, then that would mean a patent claim using such a term as "for" would be invalid. Looking to U.S. Patent No. 6,105,134 we find in claim 4:

> 4. A head end transmitter **for creating** verifiable programming information that is transmitted within a cable television system, the head end transmitter comprising:
> a control word generator **for generating** a control word;

a device **for securely maintaining** a shared secret;

a processor **for performing** a secure hash function having inputs of said control word, said shared secret, and said programming information, **for creating** a source authentication from at least a portion of an output from said secure hash function; and

a transmitter **for transmitting** said source authentication, said programming information, and said control word.

Additionally, we refer the Examiner to MPEP §706.03(d) "Rejections Under 35 U.S.C. 112, Second Paragraph - 700 Examination of Applications"

With respect to the rejection of claims under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention, the Examiner guideline states:

Examiner Note

1. This rejection must be preceded by form paragraph 7.30.02 or 7.103.2. This form paragraph should be followed by one or more of the following form paragraphs 7.34.02 - 7.34.11, as applicable. If none of these form paragraphs are appropriate, a full explanation of the deficiency of the claims should be supplied. Whenever possible, identify the particular term(s) or limitation(s) which render the claim(s) indefinite and state why such term or limitation renders the claim indefinite. **If the scope of the claimed subject matter can be determined by one having ordinary skill in the art, a rejection using this form paragraph would not be appropriate.** See MPEP §§ 2171 - 2174 for guidance.

The Examiner should provide the Applicant with an explanation showing that one of ordinary skill in the art could not determine the scope of the claimed subject matter.

With regard to the Examiner's indication that the claims are "indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention," we refer the Examiner to MPEP §2172, which clear provides the guideline:

> A rejection based on the failure to satisfy this requirement is appropriate only where applicant has stated, somewhere other than in the application as filed, that the invention is something different from what is defined by the claims. In other words, the invention set forth in the claims must be presumed, in the absence of evidence to the contrary, to be that which applicants regard as their invention. *In re Moore*, 439 F.2d 1232, 169 USPQ 236 (CCPA 1971).

The Applicant contends that the claims clearly point out and distinctly claim the subject matter **which applicant regards as the invention**. The Examiner has not provided evidence that the Applicant has stated, somewhere other than in the application as filed, that the invention is something different from what is defined by the claims.

Evidence that shows that a claim does not correspond in scope with that which applicant regards as applicant's invention may be found, for example, in contentions or admissions contained in briefs or remarks filed by applicant, *Solomon v. Kimberly-Clark Corp.*, 216 F.3d 1372, 55 USPQ2d 1279 (Fed. Cir. 2000); *In re Prater*, 415 F.2d 1393, 162 USPQ 541 (CCPA 1969), or in affidavits filed under 37 CFR 1.132, *In re Cormany*, 476 F.2d 998, 177 USPQ 450 (CCPA 1973). The content of applicant's specification is not used as evidence that the scope of the claims is inconsistent with the subject matter which applicants regard as their invention. As noted in *In re Ehrreich*, 590 F.2d 902, 200 USPQ 504 (CCPA 1979), agreement, or lack thereof, between the claims and the specification is properly considered only with respect to 35 U.S.C. 112, first paragraph; it is irrelevant to compliance with the second paragraph of that section.

The Examiner erroneously holds that such phrases as "responding to...", "transmitted to...", "for generating...", for receiving...", etc. make the claims indefinite and unclear in that neither means nor interrelationship of means nor method steps are set forth in the claims in order to achieve the

desired results expressed the phrases.

The Examiner's holding is too broad because it fails to particularly point out where each offending phrase can be found in each claim. That is, the Examiner has given a blanket rejection of all the claims by stating "Throughout claims 70-94. . ." (see page 4 of the Office action).

Looking to claim 70, for example, we find **no** instance of the phrase "responding to . . .," or the phrase "transmitted to . . ."

Looking to claim 71, for another example, we find the phrase *a key generation algorithm responsive to said key information* ***for generating a user key***. Claim 71 depends from claim 70 which clearly points out that the *service server* transmits *said key information* in a header to *said terminal unit.*

Accordingly, it is respectfully requested that the Examiner identify each particular claim deemed to be indefinite and identify by line number where the offending term or phrase can be found.

On page 5 of Paper No. 19, the Examiner quotes a phrase "a host server responding to said identity characters . . .". The Examiner does not identify which claim contains the foregoing phrase, yet indicates that it is not clear how the relationship between the host server and a service server is being done [?] with respect to the foregoing phrase. Since the foregoing phrase does not include the term "service server" we wonder what the Examiner means.

The specification teaches the invention and discloses, Service server 22 transmits to host server 23 a request signal that asks for key information that corresponds to the identity characters transmitted by the user from terminal unit 20. In response to reception of the request signal, host

server 23 transmits the key information to the service server 22, and the key information is then transmitted to terminal unit 20. Service server 22 also transmits the key information to terminal unit 20 in response to the user's request. The host server 23 generates the key information corresponding to the identity characters transmitted from service server 22 and stores the key information together with the identity characters, and then transmits the key information to service server 22 in response to the request signal generated by service server 22.

The Examiner has referred us to the first paragraph of claim 79, stating "it is not clear 'receiving' is from what entity, is the receiving is the same receiving transmitted from the server service in paragraph two or is from another entity."

Looking to claim 79, set forth in the first paragraph (first feature) is *a terminal unit having a decryption algorithm, said terminal unit transmitting identity characters of a user, receiving and storing a key information, receiving a protocol including encrypted digital content, and decrypting said protocol by using said decryption algorithm and said key information.*

One of ordinary skill in the art would easily recognize, in light of the disclosure (claims are not to be read in a lexicographic vacuum), that the invention is directed towards receiving data over, for example, the Internet. Accordingly, it is not of particular importance to the invention what entity provides, for example, the *key information* received by the *terminal unit*. However, when reading the claim **as a whole** (not individual bits and pieces of the claim) as required, it is clearly pointed out that *a service server* transmits *said key information to said terminal unit.*

Accordingly, claim 79 clearly interrelates essential elements of the invention as defined by the specification, and clearly points out to one of ordinary skill in the art that the invention comprises

at least the terminal unit, the service server, encryption and decryption algorithms, and the corresponding functions of the terminal unit and service server.

The Examiner has indicated that "it is not clear that encrypted digital content is part of the protocol or is attached to non-encrypted protocol" with respect to claim 79. Claim 79 states, in part, *a protocol including encrypted digital content.* The word "including" is to be construed in context of specification and drawings, not in lexicographic vacuum. See *In re Hoch,* 428 F.2d 1341, 166 USPQ 406, 407 ftnt 3 (CCPA 1970); *Ex parte Mowa,* 31 USPQ2d 1027, 1028 ftnt 1 (1993), *Ex parte Raske*, 28 USPQ2d 1304 (1993), and *Ex parte Hiyamizu,* 10 USPQ2d 1393 (1988).

Additionally, it is not permitted to read limitations into a claim. Since there is no claim to "non-encrypted protocol" the Examiner has no reason to question whether "encrypted digital content . . . is attached to non-encrypted protocol."

In general, the specification clearly defines the invention as having a copyright protection protocol wherein digital information that has been encrypted is added to a header. Accordingly, the protocol received by the terminal unit includes encrypted digital content as set forth in claim 79. The phrase *a protocol including encrypted digital content* in claim 79 does not provide any other undisclosed meaning.

C. Claims 20-27, 29 and 70-94 were rejected under 35 U.S.C. §102(e) as being anticipated by Pinder et al. '134 (*hereafter*: Pinder). The applicant respectfully traverses this rejection for the following reason(s).

Note that in order for an anticipation rejection to be proper, the anticipating reference must disclose exactly what is claimed. "A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). "The identical invention must be shown in as complete detail as is contained in the ... claim." *Richardson v. Suzuki Motor Co.*, 9 USPQ2d 1913, 1920 (Fed. Cir. 1989). Note here that the Examiner has not relied on "inherency," accordingly, each and every element must be expressly described in Pinder.

Amended claim 20 calls for, in part, *a protocol format generator located at a server location, said protocol format generator generating a copyright protection protocol by utilizing key information generated in response to identity characters of a user transmitted to said server location from a terminal unit.*

Pinder fails to disclose *identity characters of a user transmitted to said server location from a terminal unit*, and more particularly fails to disclose *utilizing key information generated in response to identity characters of a user transmitted to said server location from a terminal unit* as amended.

In Paper No. 19, the Examiner refers us to col. 12, lines 47-58 in this regard. Here, Pinder discloses "FIG. 4 also shows how the techniques used to ensure the security of EMMs are also used to ensure the security of messages sent from DHCT 333. The example shown in FIG. 4 is a forwarded purchase message (FPM). The forwarded purchase message is used for the interactive purchase of an instance of a service. One example of such a purchase is what is called impulse pay-per-view, or IPPV. In such a system, the beginning of an event, for example, a baseball game,

is broadcast generally and customers can decide whether they want to see all of it. In that case, **they must provide input to DHCT 333 that indicates that they wish to see the entire event."**

Accordingly, there is no disclosure in the cited section of Pinder, quoted above, that discloses *identity characters of a user transmitted to said server location from a terminal unit*, and more particularly *utilizing key information generated in response to identity characters of a user transmitted to said server location from a terminal unit.* That is, the input to DHCT (digital home communications terminal) 333 that indicates that one wishes to see the entire event is not disclosed to be *identity characters of a user.*

Therefore, absent some showing that at least the foregoing features of claim 20 are disclosed by Pinder, the rejection is deemed to be in error and should be withdrawn.

Applicant has reviewed Pinder further, and finds no mention of *identity characters of a user*, nor any equivalency thereto. According to the present invention *identity characters of a user* may be, for example, a social security number or a drivers licence number. The advantage of utilizing *identity characters of a user* is that the user is not limited to a particular playback apparatus or personal computer for receiving downloaded digital information.

Pinder, on the other hand, discloses in column 42 that "When a user of a DHCT 333 wishes to purchase an instance of a service offered by an EA, the user sends a purchase order to the EA with the serial number (which is also the IP address) of the DHCT 333." The DHCT 333 is not a user, but is instead a particular apparatus. Accordingly, the serial number of the DHCT 333 is not equivalent to *identity characters of a user.*

Note that if an unauthorized user of digital home communications terminal 333 gains access

to the network to download digital information, the authorized user gets the bill even thought the authorized user did not request the information. The present invention has the advantage that only the authorized user of the digital home communications terminal 33 will be able to download information.

Claim 20 also calls for, in part, *a protocol format decoder located at said terminal unit, said protocol format decoder having a decryption algorithm, said protocol format decoder storing the key information generated by the protocol format generator, said protocol format decoder decrypting and replaying the digital contents according to the stored key information and the information of the header received from the protocol format generator.*

Pinder fails to disclose the foregoing feature of the present invention.

Accordingly, the rejection of claim 20 is deemed to be in error and should be withdrawn.

We note here that the Examiner fails to identify any particular parts of Pinter upon which the rejection is based. Note, *Ex parte Levy*, 17 USPQ2d 1461, 1462 (1990) states:

> "it is incumbent upon the examiner to identify wherein each and every facet of the claimed invention is disclosed in the applied reference."

Additionally, the Examiner is referred to 37 CFR §1.104(c)(2) which directs the Examiner to designate the particular part relied on as nearly as practicable, when a reference is **complex** or

shows or describes inventions other than that claimed by the applicant.

Like claim 20, claim 23 calls for *generating key information using random numbers, said key information corresponding to identity characters of a user transmitted to said server location from a terminal unit*, thus claim 23 is deemed not to be anticipated by Pinder. Also, claim 25 calls for *key data being randomly generated in response to identity characters of a user transmitted to a host server from a terminal unit*, and since Pinder fails to disclose *identity characters of a user*, the foregoing feature of claim 25 is not disclosed by Pinder.

Claims 70, 79 and new claim 95 also call for *identity characters of a user* and use these characters to generate key information. Since Pinder fails to disclose *identity characters of a user*, and fails to disclose generating key information in response to the user's identity characters, claims 70, 79 and new claim 95 are not anticipated by Pinder.

Additionally, claim 23 calls for, in part, *said protocol format generator applying said key information to a key generating algorithm to generate a user key utilized to generate a temporary validation key, said temporary validation key being encrypted to generate user authorization information, said header including said user authorization information.*

The Examiner fails to identify where the foregoing features is disclosed in Pinder, and the applicant can find no such disclosure.

Further, claim 23 calls for, in part, *said protocol format decoder generating a second user key in response to the received key information, analyzes said user authorization information in*

response to said second user key to determine whether the user is authorized to receive said encrypted digital information, and when said user is authorized to receive said encrypted digital information, utilizing said second user key to decrypt said temporary validation key from said user authorization information, the decrypted temporary validation key being used to decrypt said encrypted digital information.

Pinder fails to disclose a method or apparatus for determining whether a **user** is authorized, but instead determines if an apparatus, *i.e.,* DHCT 333, is authorized to receive the service instance (325). If it is, control word 319 is used in service decryptor 347 to decrypt encrypted content to produce original content 325.

There is no disclosure in Pinder of *generating a second user key in response to the received key information*, no disclosure of *utilizing said second user key to decrypt said temporary validation key* and no disclosure of *the decrypted temporary validation key being used to decrypt said encrypted digital information*. As noted above, Pinder discloses that a "control word 319 is used in service decryptor 347 to decrypt encrypted content to produce original content 325." generated control word 319 is used to encrypt service instance 325 and generating the ECM 323 which carries the information needed to decrypt the service instance to DHCT 333. The control word 319 is generated by random number generator 317. This can be a true random number generator, whose output is the result of some basic underlying random physical process, or some other means, for example, the result of encrypting a value, called a "counter" (which increments by one after each use) with 3DES, using the MSK as the key.

Accordingly, Pinder's invention is not the same as the Applicant's invention. Thus the rejection is deemed to be in error and should be withdrawn.

Claim 22 requires, in part, that the protocol format generator *generates a user key by adding the key information to a key generation algorithm and calculates a hash value by adding the user key to a hash algorithm*, and *encrypting a temporary validation key by using the user key.* Also claim 22 requires that the header include *user authorization information with the hash value and the encrypted temporary validation key.*

The Examiner refers us to col. 6, lines 29-63 of Pinder, where there is discussion of an (encrypted) control word (CW) 202, a Multi-Session key (MSK) 208 and a message authentication code using a keyed-hash value derived from the message content combined with a secret (all or part of MSK 208). The Examiner also refers us to col. 20, lines 28-43, which provides teachings similar to col. 6, lines 29-63.

Control word (CW) 202 is generated by control word Generator 203 which can be either a physically random number generator or can use a sequential counter with a suitable randomization algorithm to produce a stream of random CWs, and the CW 202 is encrypted for transmission. The Examiner equates CW 202 to the *temporary validation key*. Claim 22 calls for *encrypting a temporary validation key by using the user key*, wherein the user key is generated by adding the key information (generated in response to identity characters of a user) to a key generation algorithm.

Pinder's control word is preferably encrypted using a symmetric cipher such as the Triple-DES algorithm using two distinct 56-bit keys (which taken together comprise MSK 208). Note that MSK 208 is provided by Multi-Session Key generator 205 and there is no further disclosure of Multi-Session Key generator 205 in Pinder.

Thus, Pinder's MSK 208 is not generated by adding the key information (generated in response to identity characters of a user) to a key generation algorithm. Accordingly, MSK 208 is

not equivalent to the claimed *user key* which is generated by adding the key information (generated in response to identity characters of a user) to a key generation algorithm.

Accordingly, claim 21 is not anticipated by claim Pinder.

Claim 22 requires that *the protocol format decoder generates a user key by adding the stored key information to a key generation algorithm and decrypts a temporary validation key, transmitted within said copyright protection protocol, by using the user key, said protocol format decoder decrypting the encrypted digital contents with the temporary validation key, said key information being formed to correspond to said identity characters of the user.*

Again, the stored key information *correspond to said identity characters of the user*, which is not disclosed by the Pinder.

Pinder discloses Encrypted multi-session key E_{Kpr} (MSK) is decrypted in decryptor 234 using DHCT private key from memory 232 to provide multi-session key MSK. Demultiplexer 230 also selects from transport data stream TDS encrypted control word (CW) E_{MSK} (CW). The encrypted CW is processed in decryptor 236 using multi-session key MSK as the decryption key to provide the unencrypted CW. The unencrypted CW preferably changes at a high rate, for example, once every few seconds. Demultiplexer 230 also selects from transport data stream TDS encrypted service E_{CW} (SERVICE). The encrypted service is processed in decryptor 238 using the CW as the decryption key to recover the unencrypted service.

Accordingly, we now must consider whether Pinder's DHCT private key corresponds to the claimed *stored key information*. The Applicant finds no disclosure in Pinder that teaches that the DHCT private key *correspond to . . . identity characters of the user*, nor that the DHCT private key

is transmitted from a server location to a terminal unit to be stored in memory 232.

"There must be no difference between the claimed invention and the reference disclosure, as viewed by a person of ordinary skill in the field of the invention." *Scripps clinic & Research Foundation v. Genentech, Inc.*, 927 F.2d 1565, 18 USPQ2d 1001, 18 USPQ2d 1896 (Fed. Cir. 1991).

Accordingly Pinder fails to anticipate claim 22.

The remaining pending claims are deemed to be patent able over Pinder at least for the reasons discussed above.

D. Claims 28, 30 and 31 were rejected under 35 U.S.C. §103(a), as rendered obvious and unpatentable, over Pinder in view of Ginter et al. (*hereafter*: Ginter). The Applicant respectfully traverses this rejection for the following reason(s).

Ginter fails to teach at least the feature of claim 25, i.e., *key data being randomly generated in response to identity characters of a user*, noted above as not being disclosed by Pinder. Accordingly, claims 28, 30 and 31 are deemed to be patentable for the same reasons as claim 25.

E. The patentability of new claim 95 has been discussed above. Additionally, new claim 98, for example calls for comparing a hash value in said header to a generated second hash value in the decryptor, and when the second hash value is determined to coincide with the hash value in the header, the user is recognized to be authorized and then the temporary validation key is decrypted

using the user key.

Accordingly, claims 95-98 are not anticipated by Pinder and are not obvious in view of the combined teachings of Pinder and Ginter.

The Examiner is respectfully requested to reconsider the application, withdraw the objections and/or rejections and pass the application to issue in view of the above amendments and/or remarks.

Should a Petition for extension of time be required with the filing of this Amendment, the Commissioner is kindly requested to treat this paragraph as such a request and is authorized to charge Deposit Account No. 02-4943 of Applicant's undersigned attorney in the amount of the incurred fee if, **and only if**, a petition for extension of time be required **and** a check of the requisite amount is not enclosed.

Respectfully submitted,

Robert E. Bushnell
Attorney for Applicant
Reg. No.: 27,774

1522 K Street, N.W.
Washington, D.C. 20005
(202) 638-5740

Folio: P55501
Date: 1/27/04
I.D.: REB/MDP